

EXHIBIT 1

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

‘163 C1 Patent: Claim 1	Method and System for Demultiplexing a First Sequence of a Packet, Components to Identify Specific Components, Wherein Subsequent Components Are Processed Without Re-Identifying Components
1. Preamble. A method in a computer system for processing a message having a sequence of packets,	<p>Juniper Networks, Inc. provides networking products, in the form of equipment and software, specializing in the field of Ethernet and IP networking. Juniper supplies a number of different types of products for constructing these networks, depending on the location or function in the network.</p> <p>For security functions in the network, the accused Juniper products utilize Intrusion Detection and Prevention (IDP), and Unified Threat Management (UTM). IDP functions are also known as “Deep Inspection”, or as “Intrusion Detection System” (IDS), or as “Intrusion Prevention System” (IPS). UTM functions are also known as Network Anti-Virus, Network Anti-Spam, Web Filtering, or Content Filtering.</p> <p>The accused functionalities are present in appliances, switches, routers, and modules of the SRX Series, J Series, NetScreen Series, ISG Series, SSG Series, and IDP Series. The accused products have these features implemented as part of/in conjunction with the embedded Operating System, Junos OS, and, for IDP, as a non-Junos but stateful, flow based processing system.</p> <p><u>Technical Overview</u></p> <p>Juniper’s networking operating system, Junos, offers flow based routing. Junos drives many (but not all, see Appendix A to Implicit’s disclosure) of the accused products here, e.g., the J-Series and SRX routers, mentioned above. Flow based processing is central to managing the network data flow, including ensuring network security.</p> <p>Flow based processing turns on the creation of “sessions.” A session is a unique flow, e.g. an FTP connection between a client and a server. A session is created to store the security measures to be applied to the packets of the flow, to cache information about the state of the flow, to allocate required uses for the flow, and to provide a framework for features such as Application Layer Gateways (“ALG’s”) and firewalls.</p> <p>In Juniper’s flow based processing, the system inspects the first packets of a flow, determines the processing appropriate for that flow, and then accomplishes that processing for all subsequent packets identified as belonging to that flow. To accomplish this, the system maintains state by flow.</p>

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

By methodological step, Juniper's flow based processing works as follows:

When a packet arrives at the system, it is classified according to multiple classification criteria, e.g., source address, destination address, source port, destination port, and other such classification characteristics. This can often be a greater than a five tuple classification process. If this process identifies the packet as the first packet of a new flow, as against a packet belonging to a flow already transverse the system (*see below*), the system undertakes a policy look-up to determine what actions need to be taken, *i.e.*, what processing steps should be taken as to that particular flow. Each separate service, e.g. firewall, or antivirus, has a separate policy look-up.

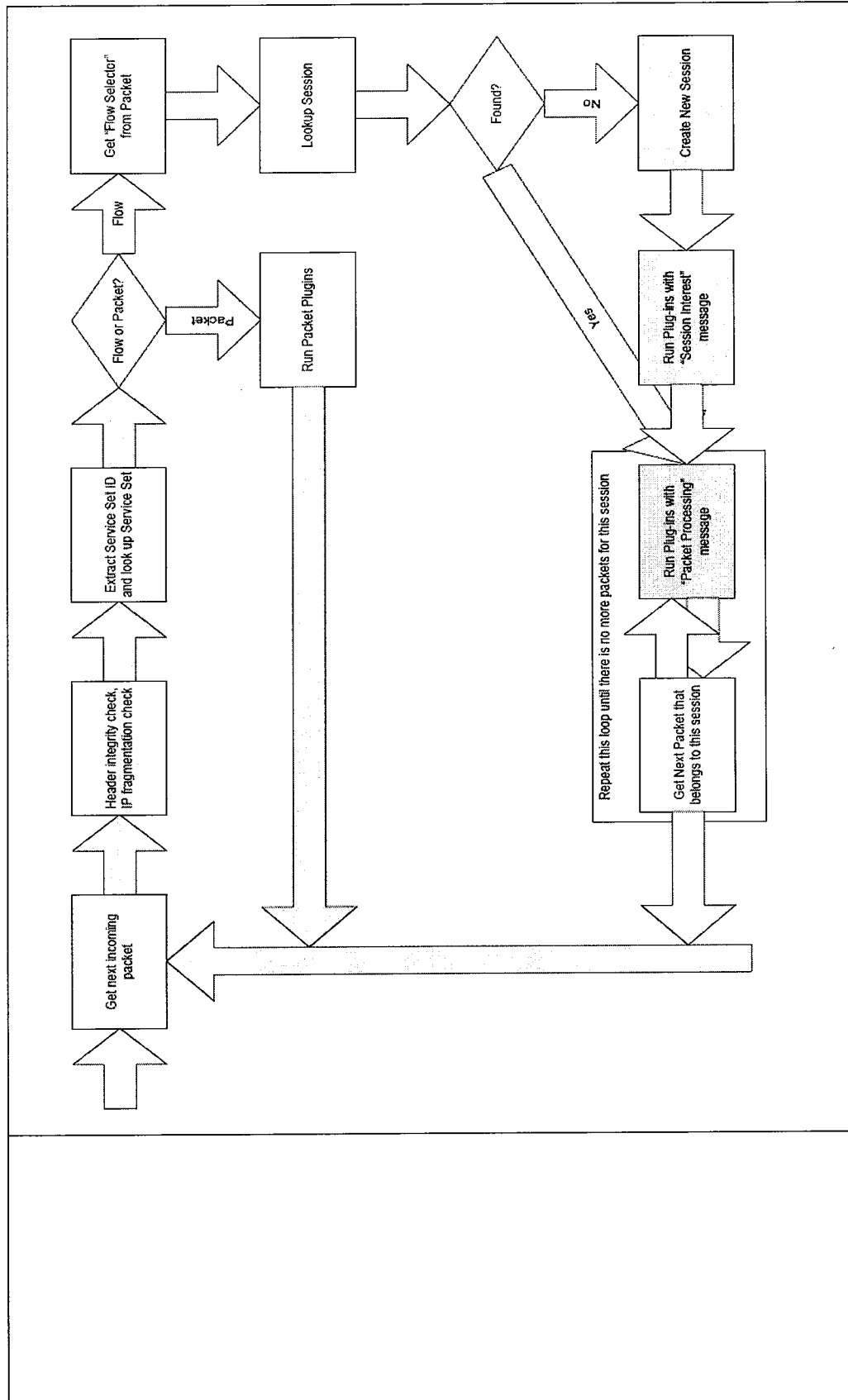
The processing steps called for by the policies are captured in independent C-file modules. The system comes with modules (actions) loaded, and the policies call out which modules (actions) will be taken for a particular flow. In this fashion, the system determines which actions (processing steps) should be taken and which not.

After the policy look-ups are undertaken for the first packet, the actions to be taken are stored in the data structure called a flow state. The status of one particular flow is called a flow state; the status of all of the flows transverse the system is held in a data structure known as a flow table. When subsequent packets of the same flow arrive, they are classified, associated with the existing flow state, and the actions performed on the first packet are subsequently performed on the subsequent packets. The actions to be taken are stored as data structures in memory, post-first packet inspection. In this way, the policy look-up need not occur on a recursive packet-by-packet basis for a given flow.

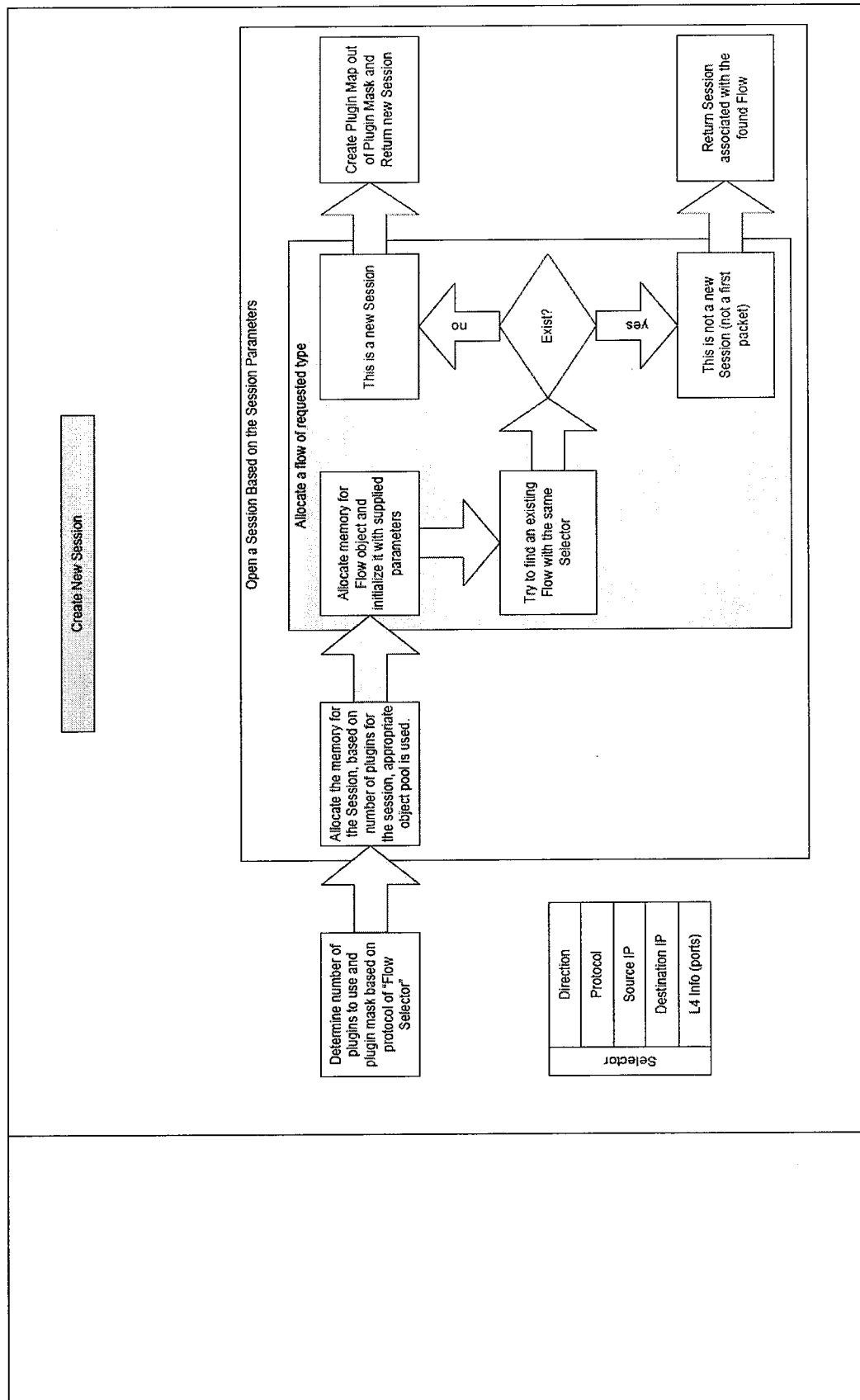
In the Junos architecture, policies can be changed dynamically at run-time without shutting down the system, recompiling the kernel, and spooling the system up. Indeed, the system is designed to be modular, extensible, and changeable at run-time.

To depict it graphically, following are the basic flow based processing steps:

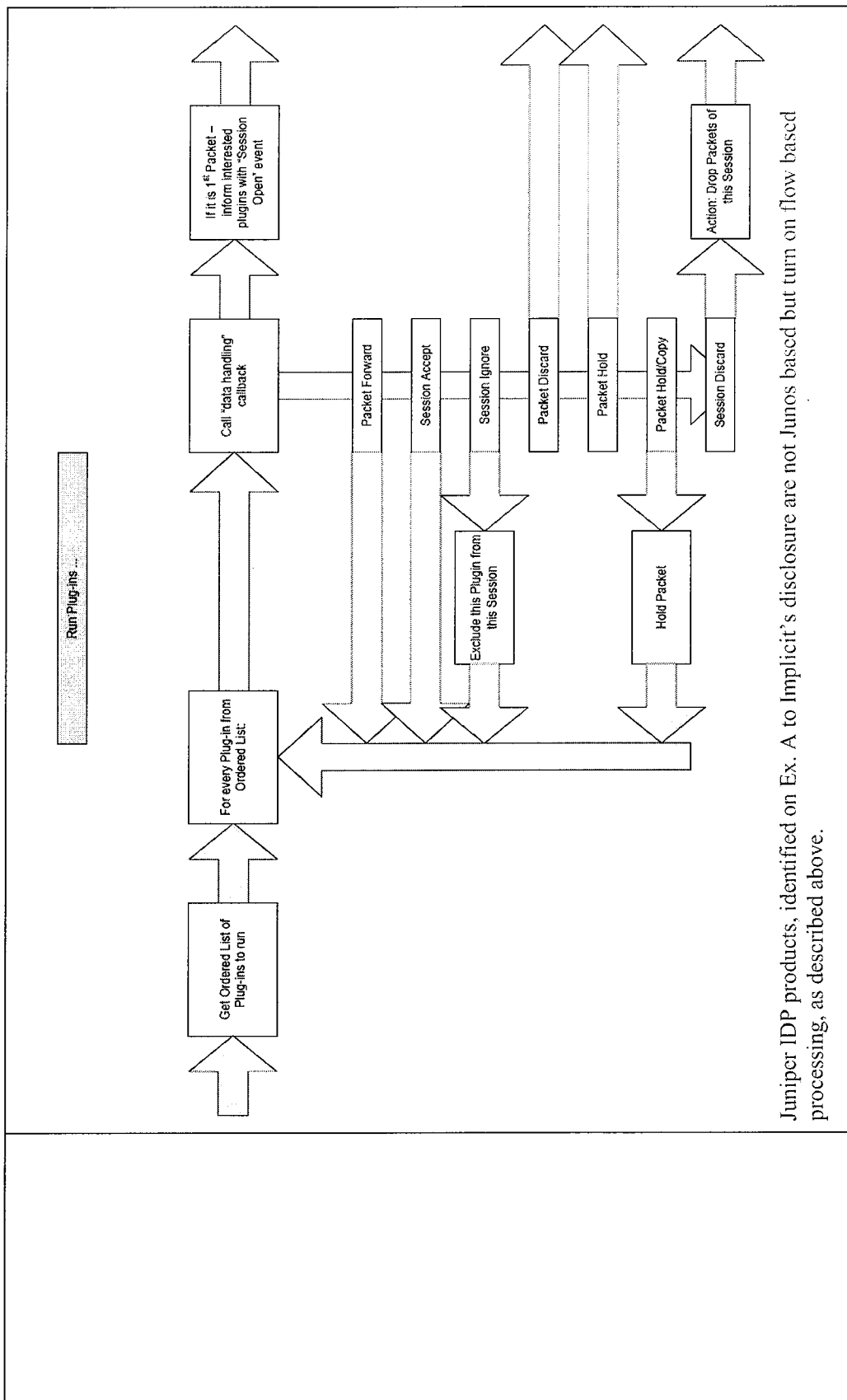
Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing



Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing



Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing



juniper

SECURITY PRODUCTS COMPARISON MATRIX

[illegible][illegible]

Source: *Security Products Comparison Matrix*. Published by Juniper Networks, Inc., November 2010, <http://www.juniper.net/us/en/local/pdf/datasheets/1000265-en.pdf>

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

Evidence '163 C1 Pre(2)

Juniper's SRX product, accused here, offers flow based processing.

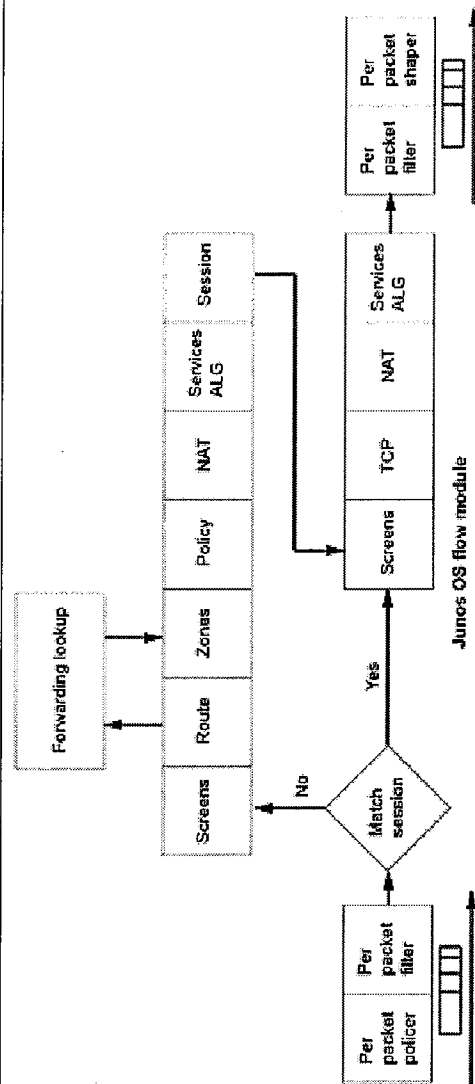
Junos OS for SRX Series Services Gateways integrates the world-class network security and routing capabilities of Juniper Networks.

Junos OS includes a wide range of packet-based filtering, class-of-service (CoS) classifiers, and traffic-shaping features as well as a rich, extensive set of flow-based security features including policies, screens, network address translation (NAT), and other flow-based services.

Traffic that enters and exits services gateway is processed according to features you configure, such as packet filters, security policies, and screens. For example, the software can determine:

- Whether the packet is allowed into the device
- Which firewall screens to apply to the packet
- The route the packet takes to reach its destination
- Which CoS to apply to the packet, if any
- Whether to apply NAT to translate the packet's IP address
- Whether the packet requires an Application Layer Gateway (ALG)

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing



Flow-based packet processing treats related packets, or a stream of packets, in the same way. Packet treatment depends on characteristics that were established for the first packet of the packet stream, which is referred to as a flow.

Packet-based, or stateless, packet processing treats packets discretely. Each packet is assessed individually for treatment.

A packet undergoes flow-based processing after packet-based filters and some screens have been applied to it. All flow-based processing for a single flow occurs on a single System Processing Unit (SPU). An SPU processes the packets of a flow according to the security features and other services configured for the session.

A flow is a stream of related packets that meet the same matching criteria and share the same characteristics. Junos OS treats packets belonging to the same flow in the same manner.

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

Source: *Junos OS Security Configuration Guide*, Published by Juniper Networks, Inc., March 2011, pages 4-5, <https://www.juniper.net/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-security/junos-security-swconfig-security.pdf>

Junos for the J Series Routers also provides flow based processing:

Evidence '163 C1 Pre(3)

Junos OS for J Series Services Routers integrates the world-class network security and routing capabilities of Juniper Networks Operating System.

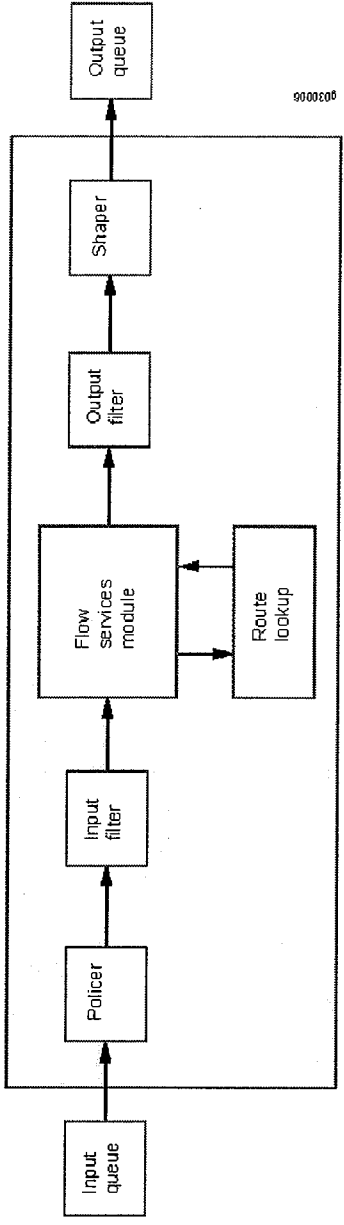
Traffic that enters and exits a services router running Junos OS is processed according to features you configure, such as security policies, packet filters, and screens. For example, the software can determine:

- Whether the packet is allowed into the router
- Which class of service (CoS) to apply to the packet, if any
- Which firewall screens to apply to the packet
- Whether to send the packet through an IPsec tunnel
- Whether the packet requires an Application Layer Gateway (ALG)
- Whether to apply Network Address Translation (NAT) to translate the packet's address
- Which route the packet uses to reach its destination

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1

Claims Chart

Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

	 <p>Packets that enter and exit a services router running Junos OS undergo both packet-based and flow-based processing. A device always processes packets discretely. Packet treatment depends on characteristics that were established for the first packet of the packet stream.</p> <p>A packet undergoes flow-based processing after any packet-based filters and policers have been applied to it.</p> <p>A flow is defined as a set of packets coming from the same source/destination addresses, source/destination ports (when applicable), protocol, and ingress/egress zones. Flows are time bound so it is possible to have packets that, while fitting the previous definition belong to different flows. For example, when an existing session is initiated and terminated, after which a new session is established using the exact same parameters as the previous session, the packets would belong to different flows.</p> <p>Source: <i>Junos OS Security Configuration Guide</i>, Published by Juniper Networks, Inc., March 2011, pages 94, https://www.juniper.net/techpubs/software/junos-security/junos-security/10.2/junos-security-swconfig-security/junos-security-swconfig-security.pdf</p>
<p>1a. the method comprising: providing a plurality of components, each component being a</p>	<p>As described in the technical overview above, the accused products offer flow based processing, wherein a series of actions (modules) are instantiated as a stateful processing path, post-first packet inspection. The accused products provide components which operate on the data in sequence, with the output of one component being the input of the</p>

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

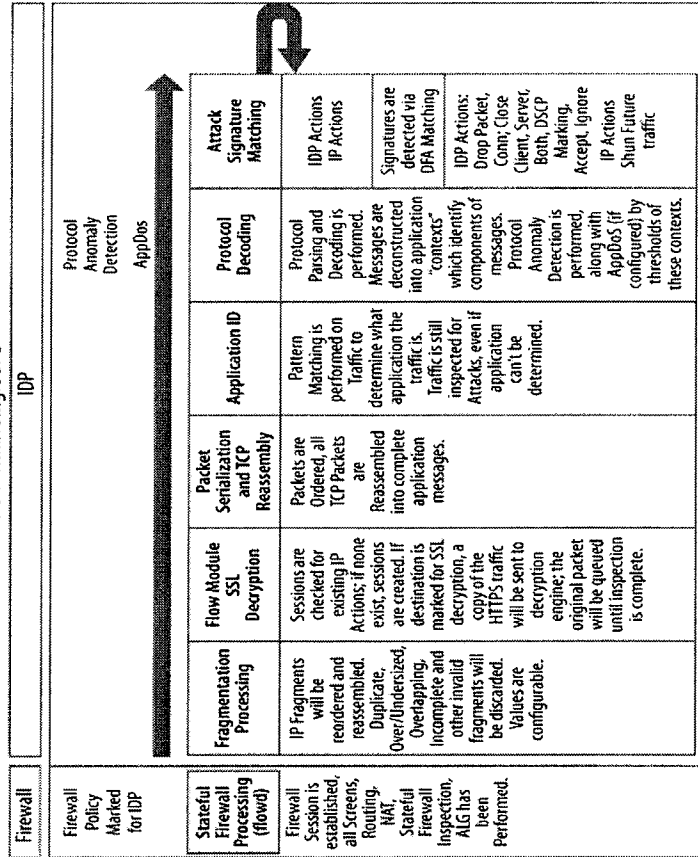
software routine for converting data with an input format into data with an output format;

next. They also perform IPS algorithm processing.

Evidence '163 C1 1a(1)

IDP Packet Processing Walkthrough

View within Single SPU



Within the IPS engine there are several stages of processing, as illustrated above. IPS processing on the SRX can be broken down into eight general stages of processing:

Stage 1: Fragmentation processing

11

CONTAINS INFORMATION DESIGNATED "HIGHLY CONFIDENTIAL" BY JUNIPER

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

The first thing that must happen before you can really get to the inspection is that the SRX must process fragmented traffic (if present). To ensure that common IDS evasion techniques using fragmentation are not effective, it rebuilds any fragmented traffic from a Layer 3 perspective. This stage also provides countermeasures against fragment-based attacks such as missing fragments, underlapping or overlapping fragments, duplicate fragments, and other fragment-based anomalies. Many of these values are also configurable in the IPS sensor configuration section, although defaults should suffice in most cases.

Stage 2: IPS flow setup

After any Layer 3 fragments are processed, the SRX examines the traffic to see whether it has an existing session for it or if there is an existing session which might need some special processing. The IPS session table is different from the firewall session table, because additional IPS state related to the traffic is required.

Stage 3: SSL decryption (if applicable)

If SSL decryption is configured, and traffic is destined to a web server that is configured to be decrypted, decryption happens in this phase.

Stage 4: Serialization and reassembly

For accurate IPS processing, all messages must be processed in order, in a flow, and the messages must be reassembled if they span multiple packets. Without reassembly, an IPS engine can be easily evaded, which would result in lots of false positives. The SRX IPS engine ensures that before traffic is processed, it is ordered and reassembled in this stage of the processing.

Stage 5: Application identification

The SRX has the ability to detect what application is running on any Layer 4 port. This is important because it allows the device to determine what traffic is running in a given flow regardless of whether it is running on a standard port. Even if the application cannot be identified, the SRX can still inspect it as a bytestream. This stage typically happens within the first couple of kilobytes of traffic, and the SRX utilizes both directions of

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

	<p>the traffic to identify the application.</p> <p>Stage 6: Protocol decoding</p> <p>Once the application is identified (or is simply classified as a stream), the SRX decodes the application from a protocol level, a process known as protocol decoding. Protocol decoding allows the SRX to chop up the traffic into contexts, which are specific parts of different messages. Contexts are very important to IPS processing because they allow the SRX to look for attacks in the specific location where they actually occur, not just blindly by byte matching across all traffic that passes through the SRX. After all, you wouldn't want the SRX to block an email conversation between you and a peer discussing the latest exploit; you would only want the SRX to block the exploit in the precise location where it actually occurs. At the time of this writing, the SRX supports almost 600 application contexts. Contexts are one of the ways that the SRX seeks to eliminate false positives. The protocol decoding stage is also where the SRX performs protocol anomaly protection and Application Distributed Denial of Service (AppDDoS) protection, both of which we will discuss later in this chapter.</p> <p>Stage 7: Stateful signature detection</p> <p>The attack objects that rely on signatures (rather than anomaly detection) are processed in the stateful signature stage of the device's processing. These signatures are not blind pattern matches, but are highly accurate stateful signatures that not only match attacks within the contexts in which they occur, but also can be composed of multiple match criteria (using Boolean expressions between individual criteria). Typically, the attack signatures do not seek to detect a specific exploit, but rather protect against the vulnerability itself. This is important because attack exploits can vary, so writing signatures around a particular exploit is not a great tactic, but protecting against the actual vulnerability is much more powerful.</p> <p>Stage 8: IDP/IP actions</p> <p>Once an attack object in the IPS policy is matched, the SRX can execute an action on that specific session, along with actions on future sessions. The ability to execute an action on that particular session is known as an IDP action. IDP actions can be one of the following: No-Action, Drop-Packet, Drop-Connection, Close-Client, Close-Server, Close-Client-and-Server, DSCP-Marking, Recommended, or Ignore. IP actions are</p>
--	--

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

	<p>actions that can be enforced on future sessions. These actions include IP-Close, IP-Block, IP-Notify, and IP-Ratelimit.</p> <p>Source: <i>Junos Security</i>, By: Rob Cameron; Brad Woodberg; Patricio Giecco; Timothy Eberhard; James Quin; Publisher: O'Reilly Media, Inc. as part of the Juniper Networks Technical Library, September 7, 2010, ISBN-13: 978-1-4493-8171-4, pages 399-401.</p> <p>When assembled by the accused products, these components implement a variety of IDP processing algorithms.</p> <p><u>Evidence '163 C1 1a(2)</u></p> <p>Application identification Port-independent application identification enhances both security and manageability by eliminating the need to manually and comprehensively configure application-port mapping for the service objects and application objects used in the IDP rulebase and APE rulebase rules. Beginning with IDP OS Release 5.1, the application identification feature can match extended application signatures used in APE rulebase rules. Extended application signatures are also called nested application signatures. The predefined extended application signatures developed for IDP OS Release 5.1 include the most prevalent Web 2.0 applications running over HTTP.</p> <p>User-defined application signatures If the predefined signatures do not address all of your use cases, you can use the NSM Object Manager to create custom application signatures.</p> <p>Application policy enforcement The application policy enforcement (APE) rulebase enables you to mark, limit, or drop traffic that matches application signatures.</p> <p>Application volume tracking The application volume tracking (AVT) feature leverages Profiler functionality to collect statistics about application usage.</p> <p>Multimethod attack detection The IDP Series uses eight methods to detect malicious traffic.</p> <p>Zero-day protection The IDP rulebase attack objects detect protocol usages that violate published RFCs. Protocol anomaly detection protects your network from undiscovered vulnerabilities.</p>
--	--

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

Protocol decoding Juniper Networks Security Center (J-Security Center) provides a robust protocol detection engine that can decode more than 60 protocols and analyze and enforce proper usage in more than 500 contexts.

Recommended security policy and predefined attack objects J-Security Center provides a robust default security policy (called Recommended) and a comprehensive set of predefined attack objects (including those flagged as Recommended for various categories of attacks). The J-Security Center attack database includes more than 5500 signatures for identifying anomalies, attacks, spyware, and applications.

User-defined security policies and attack objects If you choose, you can use the default security policy or other predefined templates as a basis for your own user-defined security policy. Similarly, you can use the predefined attack objects as a basis for your own user-defined attack objects.

Active response methods J-Security Center attack objects are coded with recommended actions to take on the instant session, including drop packet, drop connection, close client, close server, and close client/server. You can rely on these or set your own. In addition, when the IDP Series device detects an attack from a particular IP address, it can block connections from the IP address for a configurable duration of time.

Passive response methods The IDP Series supports several passive responses, including logging and TCP reset.

Traffic decryption and decapsulation The IDP Series can decrypt or decapsulate traffic and then inspect the payload. We support decryption of SSL and decapsulation of GRE, GTP, IPsec ESP NULL, and MPLS traffic.

Stateful signature The IDP rulebase attack object signatures are bound to protocol context. As a result, this detection method produces few false positives.

Protocol anomaly The IDP rulebase attack objects detect protocol usages that violate published RFCs. This method protects your network from undiscovered vulnerabilities.

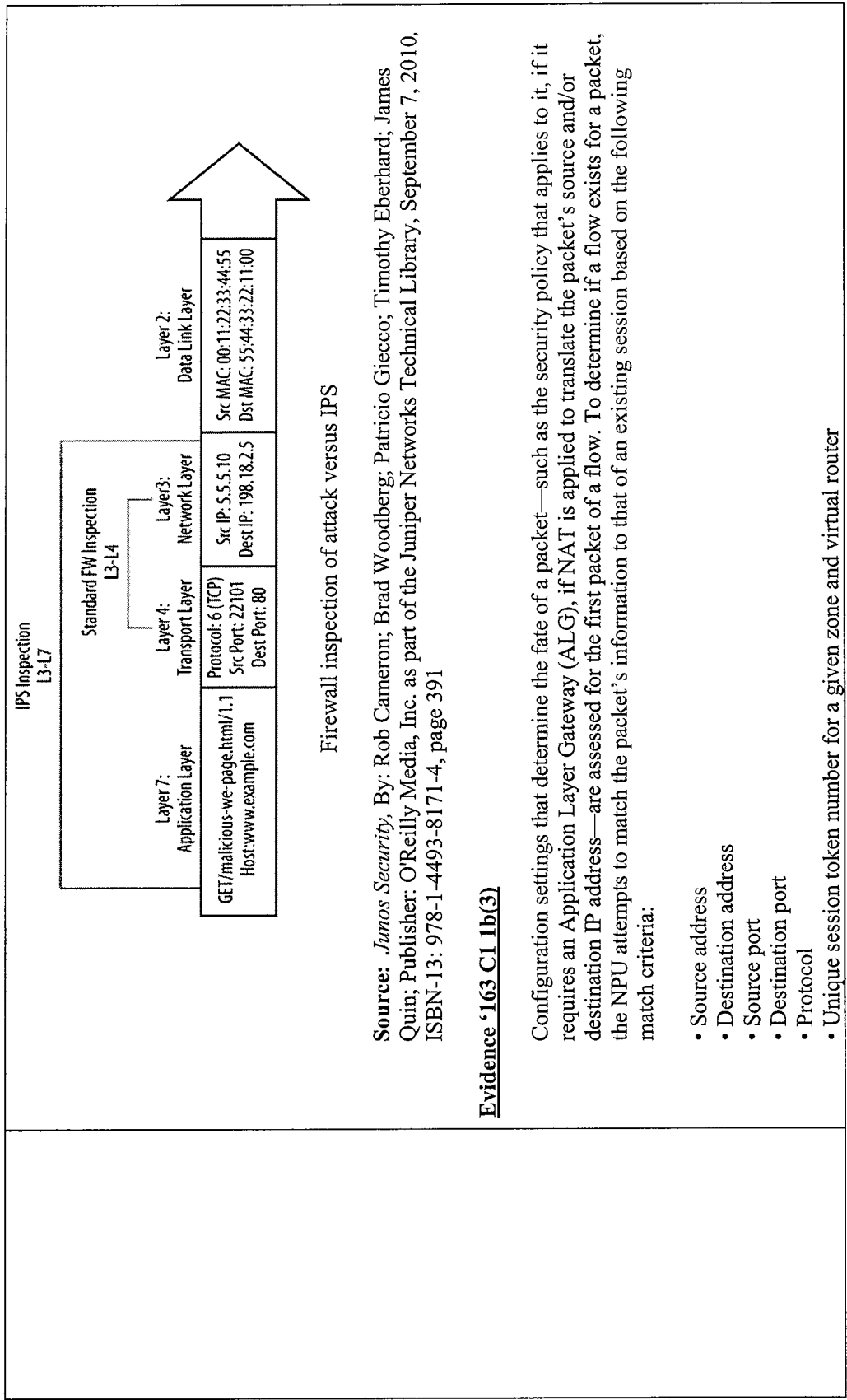
Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

	<p>Traffic anomaly The Traffic Anomalies rulebase uses heuristic rules to detect unexpected traffic patterns that might indicate reconnaissance or attacks. This method blocks distributed denial-of-service (DDoS) attacks and prevents reconnaissance activities.</p> <p>Backdoor The Backdoor rulebase uses heuristic-based anomalous traffic patterns and packet analysis to detect Trojans and rootkits. These methods prevent proliferation of malware in case other security measures have been compromised.</p> <p>IP spoofing The IDP Series device checks the validity of allowed addresses inside and outside the network, permitting only authentic traffic and blocking traffic with a disguised source.</p> <p>Denial of service (DoS) The SYN Protector rulebase provides two, alternative methods to prevent SYN-flood attacks.</p> <p>Network honeypot The IDP Series device impersonates vulnerable ports so you can track attacker reconnaissance activity.</p> <p>Source: <i>IDP Series, Concepts and Examples Guide</i>, Published by: Juniper Networks, Inc., February 2011, pages 3-7, http://www.juniper.net/techpubs/en_US/idp5.1/information-products/topic-collections/idp-5-1-rl-concepts-examples.pdf</p>
1b. for the first packet of the message, dynamically identifying a non-predefined sequence of components for processing the packets of the message such that the output format of the components of the nonpredefined sequence match the input format of the next component in the	<p>The first packet of a flow is dynamically identified using packet inspection. Based on that inspection, the accused products utilize a technique of “policy expressions,” which are script-like directives that are loaded and re-loaded into the systems while they are running. They may be loaded and re-loaded into the systems by people, other systems or software, or both. The policies direct the system to identify the processing components and algorithms which are to be applied to the network traffic which is classified through the packet inspection.</p> <p>The accused products identify a packet, look at the latest loaded and resolved policy expression which applies to that traffic/application flow, and then arrange a sequence of processing components to affect the policy expression directive. The output format of one processing step will match the input format of the next processing step. Fully custom traffic/application flow specifications, as well as fully custom processing components, can be dynamically loaded and re-loaded into the system as well. Because of the configurability of policy expressions, and traffic/applications specifications, there are near infinite resultant processing sequences – non-predefined – which will</p>

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

non-predefined sequence,	<p>execute.</p> <p><u>Evidence '163 C1 1b(1)</u></p> <p>Juniper's IPS protects the control plane and offers improved security for enhanced end-user experiences. We tightly integrate Junos OS IP technology with the most advanced security features, providing protection from a wide range of threats and attacks from both inside and outside the network, as well as supporting real-time policy assessment and enforcement.</p> <p>The Dynamic Application Awareness solution achieves these goals, providing the processing power for both stateful and stateless detection and identification of L4-L7 applications.</p> <p>Dynamic Application Awareness uses deep inspection (DI) technology to examine the L4-L7 payload via port, address, and signature detection methods.</p> <p>Residing on the MS-PIC in the M Series routers and on the MS-DPC in the MX Series routers; integrating IPS with M Series and MX Series routers.</p> <p>Source: <i>GENERATING NEW REVENUE STREAMS AND INCREASING NETWORK SECURITY Dynamic Application Awareness and Intrusion Prevention System</i>, Published by Juniper Networks, Dec, 2009, www.juniper.net/us/en/local/pdf/whitepapers/2000339-cn.pdf</p> <p><u>Evidence '163 C1 1b(2)</u></p> <p>At a high level, IPS works by scrutinizing all of the bits contained within packets to look for both known and unknown attacks.</p> <p>Traditional firewalls primarily look only at Layers 3 and 4 when it comes to security, and ignore the actual contents of the payloads themselves.</p>
--------------------------	---

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing



Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

The security policy to be used for the first packet of a flow is cached in a flow table for use with the same flow and closely related flows. Security policies are associated with zones. A zone is a collection of interfaces that define a security boundary. A packet's incoming zone, as determined by the interface through which it arrived, and its outgoing zone, as determined by the forwarding lookup, together determines which policy is used for packets of the flow.

Source: *Junos OS Security Configuration Guide*, Published by Juniper Networks, Inc., March 2011, pages 5-6, <https://www.juniper.net/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-security/junos-security-swconfig-security.pdf>

DEEP INSPECTION

Evidence '163 C1 1b(4)

A screen is a built-in tunable protection mechanism that performs a variety of security functions to keep the network safe. Screens are extremely efficient and can be tuned to operate in a small enterprise or in the largest carrier networks. Screens are widely used to add additional protections both at the edge of the network and to internal segments to protect the network from attacks and internal misconfigurations that could impact network availability. Screens are good at detecting and preventing many types of malicious traffic. Screen checks take place very early in packet processing to make mitigation as efficient and fast as possible. Although they take more processing power than a firewall filter, they are able to look deeper into the packet and at the entire session flow, essentially enabling the SRX to block very large and complex attacks. On the higher-end SRX models, many of these screens are handled in hardware, so the traffic is dropped extremely close to the ingress interface. You may notice that the screen checks take place on both the slow path and the fast path. Once a session is permitted by policy and is established, the SRX continues to monitor that connection for signs of any malicious traffic or flooding beyond its preconfigured thresholds. If it sees any malicious traffic, it blocks and drops the packets.

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

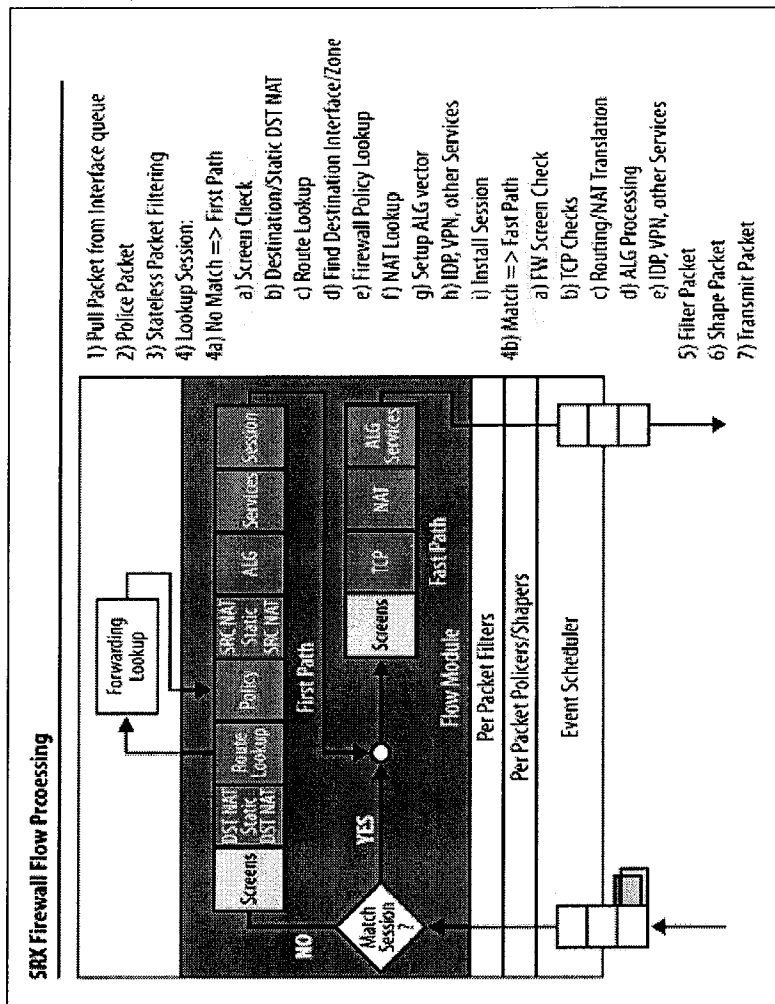


Figure 7-2. Where screen checks take place in the SRX packet flow

[from *Junos Security*. By: Rob Cameron; Brad Woodberg; Patricio Giecco; Timothy Eberhard; James Quin; Publisher: O'Reilly Media, Inc. as part of the Juniper Networks Technical Library, September 7, 2010, ISBN-13: 978-1-4493-8171-4, page 346]

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

Evidence '163 C1 1b(5)

RFC 791 states that these options are “unnecessary for the most common communications” and, in reality, they rarely appear in IP packet headers. These options appear after the destination address in an IP packet header, as shown (here). When they do appear, they are frequently being put to some illegitimate use:

Version	Header	Type of Service	Total Packet Length (in Bytes)		
Identification		Protocol	O	D	M
			Fragment Offset		
Time to Live (TTL)			Header Checksum		
Source Address					
Destination Address					
Options					
Payload					

If a packet with any of the previous IP options is received, Junos OS flags this as a network reconnaissance attack and records the event for the ingress interface.

This example shows how to detect packets that use IP screen options for reconnaissance.

Source: *Junos OS Security Configuration Guide*, Published by Juniper Networks, May 2010, Page 1025, 1028, <https://www.juniper.net/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-security/junos-security-swconfig-security.pdf>

The accused products include a generalized mechanism for doing packet inspection/flow classification.

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

Evidence '163 C1 1b(6)

Application identification supports user-defined custom application signatures for applications and nested applications. With custom application signatures, you can create signatures that will detect applications that are not part of the predefined application package.

Source: *Junos OS Security Configuration Guide, Juniper Networks, May 2010, Page 1025, 1028,*
<https://www.juniper.net/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-security/junos-security-swconfig-security.pdf>

The accused products also support inspection/classification of encapsulated or encrypted traffic.

Evidence '163 C1 1b(7)

Generic Routing Encapsulation (GRE) is a tunneling protocol designed to encapsulate a wide variety of network layer packets inside IP tunneling packets. The original packet is the payload for the final packet. The protocol is used on the Internet to secure virtual private networks. To inspect the payload of an encapsulated packet, the IDP process engine must decapsulate it. IDP Series devices support decapsulation for IP-in-GRE and PPP-in-GRE.

GPRS Tunneling Protocol (or GTP) is an IP-based protocol used within Global System for Mobile communication (GSM) and Universal Mobile Telecommunications System (UMTS) networks. To inspect the payload of an encapsulated traffic, the IDP process engine must decapsulate it. IDP Series devices support decapsulation for UDP GTPv0 and GTPv1.

Internet Protocol Security (IPsec) virtual private networks use the Encapsulated Security Payload (ESP) protocol and the NULL encryption algorithm to ensure the authenticity, integrity, and confidentiality of IP packets. To inspect the payload of an encapsulated packet, the IDP process engine must decapsulate it. IDP Series devices support decapsulation for IPsec ESP NULL traffic.

Multiprotocol Label Switching (MPLS) is an IP label switching technology that enables predetermined paths to specific destinations, called Label Switched Paths (LSPs), to be established through an inherently

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

	<p>connectionless IP network. In MPLS networks, packets contain short labels that describe how to forward them through the network. With MPLS decapsulation enabled, the IDP engine can inspect the IPv4 payload and pass through non-IPv4 payload.</p> <p>Secure Sockets Layer (SSL) is a cryptographic protocol that adds security to TCP/IP communication. Several versions of the SSL and Transport Layer Security (TLS) protocols are in widespread use in applications like Web browsing, electronic mail, Internet faxing, instant messaging, and voice over IP (VoIP). SSL and TLS encrypt the Transport Layer protocol datagrams that carry the payload of these communications. While encryption is an excellent way to keep private data from prying eyes, without inspection by the IDP Series device, it also unwittingly opens a network to dangerous viruses, trojans, or network attacks. To inspect the HTTP payload of HTTPS traffic, the IDP Series device must decrypt the HTTPS session. Your security policy can examine both the SSL session and the decrypted HTTP payload.</p> <p>Source: <i>IDP Series Concepts and Examples Guide, Juniper Networks, Published Feb. 2011</i>, http://www.juniper.net/techpubs/en_US/idp5.1/information-products/topic-collections/idp-5-1-r1-concepts-examples.pdf, pages 177-179</p> <p><u>Evidence '163 C1 1b(8)</u></p> <p>To secure your network from new viruses and attacks, your security solution must offer multiple attack detection methods and an efficient way to use the various capabilities.</p> <p>To stay one step ahead of these attacks, you need a solution that can adapt to ever-changing security threats and allow you to do so with minimal effort.</p> <p>Juniper Networks IDP Series Intrusion Detection and Prevention Appliances with Multi-Method Detection (MMD), offers comprehensive coverage by leveraging multiple detection mechanisms. For example, by utilizing signatures, as well as other detection methods including protocol anomaly traffic anomaly detection, the Juniper Networks IDP Series appliances can thwart known attacks as well as possible future variations of the attack.</p> <p>Backed by Juniper Networks Security Lab, signatures for detection of new attacks are generated on a daily</p>
--	---

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

basis, working very closely with many software vendors.

While an IDP solution is a critical component of every enterprise security infrastructure, it also offers the benefit of streamlining your business based on the applications used in the network. In addition to identifying viruses and attacks, the Juniper Networks IDP Series can identify the application associated with the particular traffic. Application intelligence enables accurate detection and reporting of volume used by applications such as social networking, peer-to-peer, or instant messaging. Armed with the knowledge of these applications running in the network, administrators can easily manage them by limiting bandwidth, restricting their use, or changing their prioritization for the best network optimization.

By accurately identifying and prioritizing application traffic, enterprises can ensure the necessary network bandwidth for business-critical applications without banning or blocking non-business applications. If necessary, specific application traffic can be blocked altogether to meet business or regulatory compliance.

Source: *IDP Series Intrusion Detection and Prevention Appliances*, published by Juniper Networks, Oct 2009, <http://www.juniper.net/us/en/local/pdf/brochures/1500025-en.pdf>

Evidence '163 C1 1b(9)

A security policy, which can be configured from the user interface, controls the traffic flow from one zone to another zone by defining the kind(s) of traffic permitted from specified IP sources to specified IP destinations at scheduled times.

Policies allow you to **deny, permit, reject** (deny and send a TCP RST or ICMP port unreachable message to the source host), **encrypt and decrypt, authenticate, prioritize, schedule, filter**, and **monitor** the traffic attempting to cross from one security zone to another. You decide which users and what data can enter and exit, and **when and where** they can go.

Source: *Junos OS Security Configuration Guide, Juniper Networks, May 2010, Page 146*, <https://www.juniper.net/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-security/junos-security-swconfig-security.pdf>

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

Evidence '163 C1 1b(10)

There can be many dozens—or even thousands—of policies configured in various SRX devices (this number varies by platform). When packets ingress any of the devices, they are evaluated against security policies.

If a match is found then the SRX does what it was instructed to do with those packets and stops evaluating through the rest of the policies.

Security policies are at the heart of any of the firewall functions of the SRX Services Gateway platform. By default, traffic entering an interface destined to any address is going to be blocked. This is the expected default behavior, and no traffic is allowed through the SRX until you permit it to enter by using security policies.

Policy configuration entitles an IF-THEN-ELSE algorithm: IF traffic X is matched, THEN action Y is performed, ELSE drop packet (default behavior).

Matching traffic (IF statement) consists of looking at packets for the five following elements:

1. Source zone: the predefined or custom zone created from the perspective of the SRX that you are configuring.
2. Source IP: any IP address, or an address book, that specifies a host IP, or a subnet. The source selected has to match the source zone.
3. Destination zone: predefined or custom zone created from the perspective of the SRX that you are configuring.
4. Destination IP: any IP address, or an address book that specifies a host IP, or a subnet. The destination selected has to match the destination zone.
5. Application: predefined or custom service that defines the source/destination ports, protocol involved, and timeout value.

If an incoming packet matches all the previous five elements, the action (THEN statement) defines what to do with this or any other packets **matching the same combination**:

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

- deny: drops the packet (silently).
- reject: drops the packet and sends a TCP-Reset to the originator of the traffic.
- permit: permits the packet.
- log: instructs the SRX to create a log entry for matching packets.
- count: provides accounting information per session.

Source: *Day One: Deploying SRX Series Services Gateways, Junos Dynamic Services Series*, published by Juniper Networks, Jan 2011, pages 54, 55, <http://www.juniper.net/us/en/community/junos/training-certification/day-one/dynamic-services-series/deploying-srx-series/>

The accused products not only support the “firewall” types of policies mentioned above, but they support much more complicated IDP policies. IDP policies are sometimes called “rulebases” and the traffic classification specification used to match a rulebase is often called a “signature” to reflect their more general programmability.

Evidence ‘163 C1 1b(11)

To help block malicious application-level attacks, Juniper Networks seamlessly integrates intrusion prevention across the entire product line. For central enterprise sites, data center environments and service provider networks with high volumes of throughput, the Juniper Networks ISG Series Integrated Security Gateways with IPS, Juniper Networks SRX100, SRX210, SRX220, SRX240, SRX650, SRX1400, SRX3000 line and SRX5000 line of services gateways can be deployed for application-level protection. The ISG Series and SRX Series tightly integrates the same software found on the Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to provide unmatched application-level protection against worms, trojans, spyware, and malware. More than 60 protocols are recognized including those used by advanced applications such as VoIP and streaming media.

Unmatched security processing power and network segmentation features protect critical high-speed networks against the penetration and proliferation of existing and emerging application-level threats. With multiple attack detection mechanisms, including stateful signatures and protocol anomaly, the ISG Series and SRX Series Services Gateways performs in-depth analysis of application protocol, context, state and behavior to deliver Zero-day protection.

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

Security administrators can deploy Juniper Networks AppSecure capability using deep inspection to block application-level attacks before they infect the network and inflict any damages. AppSecure utilizes advanced, high-performance detection mechanisms integrated with stateful inspection firewall, along with multiple threat inspection engines operating in parallel to accurately detect advanced persistent threats, including those found in nested applications within applications.

Source: *Integrated Firewall/VPN Platforms*, published by Juniper Networks, Nov. 2010, <http://www.juniper.net/us/en/local/pdf/brochures/1500024-en.pdf>

Evidence '163 C1 1b(12)

The IDP rulebase employs an attack object database to support two robust detection methods: stateful signatures and protocol anomalies.

A stateful signature combines an attack pattern with service, context, and other properties into a signature attack object. As a result, the IDP system does not need to expend resources inspecting huge sections of network traffic where attacks cannot possibly be, and IDP produces very few false positives.

A protocol anomaly is a deviation from protocol standards established by the Internet Engineering Taskforce (IETF) Request for Comment (RFC) process. Traffic that does not adhere to these standards is suspicious because most legitimate applications adhere to the standards, and anomalies can fairly be regarded as purposeful attempts to evade an intrusion detection system (IDS). IDP protocol-anomaly attack objects find traffic that deviates from IETF RFC standards.

When you create rules for the IDP rulebase, you specify:

- A source/destination/service match condition
- Attack objects
- Action
- Notification options

The IDP engine inspects the session beginning with the first packet to determine whether the session

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

matches a rule. If the session matches all rule settings for source, destination, service, and VLAN tag ID, the IDP system decodes the traffic and inspects the session packets for the attack objects specified in the rule.

Source: *IDP Series Concepts and Examples Guide, Juniper Networks, Published Feb. 2011*, http://www.juniper.net/techpubs/en_US/idp5.1/information-products/topic-collections/idp-5-1-1-concepts-examples.pdf, pages 91, 92

Unified Threat Management (UTM) is a term used to describe the consolidation of several security features into one platform, protecting against multiple threat types.

Evidence '163 C1 1b(13)

The security features provided as part of the UTM solution are:

- **Antispam**—E-mail spam consists of unwanted e-mail messages, usually sent by commercial, malicious, or fraudulent entities. The antispam feature examines transmitted e-mail messages to identify e-mail spam. When the device detects an e-mail message deemed to be spam, it either drops the message or tags the message header or subject field with a preprogrammed string. The antispam feature uses a constantly updated spam block list (SBL). Sophos [n.b., an outside company accessed through an algorithm which goes to a special internet site], updates and maintains the IP-based SBL.
- **Full File-Based Antivirus**—A virus is executable code that infects or attaches itself to other executable code to reproduce itself. Some malicious viruses erase files or lock up systems. Other viruses merely infect files and overwhelm the target host or network with bogus data. The full file-based antivirus feature provides file-based scanning on specific Application Layer traffic checking for viruses against a virus signature database. It collects the received data packets until it has reconstructed the original application content, such as an e-mail file attachment, and then scans this content.
- **Express Antivirus**—Express antivirus scanning is offered as a less CPU intensive alternative to the full file-based antivirus feature. The express antivirus feature, like the full antivirus feature, scans specific Application Layer traffic for viruses against a virus signature database. However, unlike full antivirus, express antivirus does not reconstruct the original application content. Rather, it just sends (streams) the received data packets, as is, to the scan engine. With express antivirus, the virus scanning is executed by a hardware pattern matching engine. This improves performance while scanning is occurring, but the level

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

of security provided is lessened.

- **Content Filtering**—Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type.
- **Web Filtering**—Web filtering lets you manage Internet usage by preventing access to inappropriate Web content.

Before you can configure most UTM features, you must first configure the custom objects for the feature in question. Custom objects are global parameters for UTM features. This means that configured custom objects can be applied to all UTM policies where applicable, rather than only to individual policies.

Source: *Junos OS Security Configuration Guide, Juniper Networks, May 2010, Page 843-844*, <https://www.juniper.net/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-security/junos-security-swconfig-security.pdf>

Evidence '163 C1 1b(14)

Configuration

The unified threat management [UTM] implementation in Junos OS leverages security policies as a central point where traffic is classified and directed to the appropriate modules for processing. In practice, a UTM policy specifying all UTM-related parameters is attached to a security policy, and matching traffic is processed by the UTM module according to the configuration of the UTM policy.

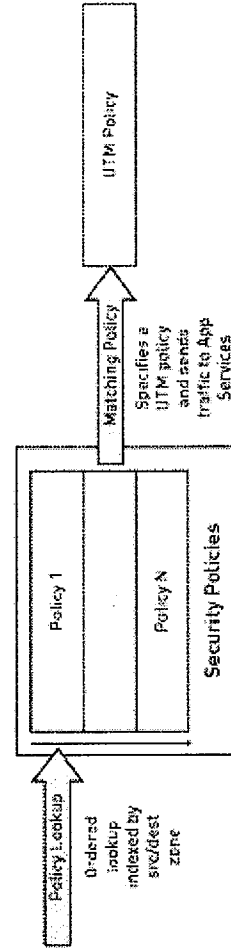


Figure 3: UTM policies

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

In a similar fashion, a UTM policy ties a set of protocols to one or multiple feature profiles. Each feature profile determines the specific configuration for each feature (antivirus, content filtering, anti-spam).

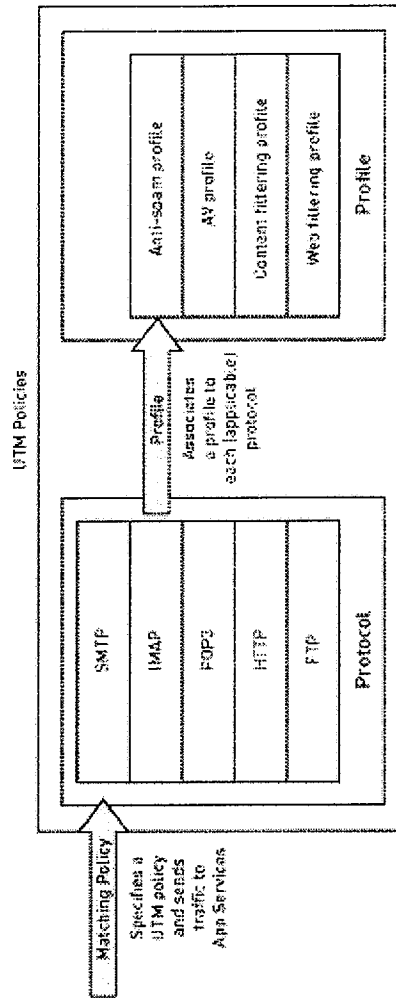


Figure 2: UTM policies and feature profiles

Source: "Application Note: Content Filtering For Branch SRX Series and J Series", JUNIPER01475161

Evidence '163 C1 1b(15)

Once a security policy specifies a UTM policy, a transparent proxy processes all matching traffic and, in the case of this book's SRX devices, modifies the contents of the traffic or generate error messages back to the user. To proxy a session, an SRX device acts both as a TCP client and as a server terminating and originating a TCP session. This uses significant resources, in terms of both memory and CPU, which puts some constraints on the total number of sessions an SRX can proxy (and, in turn, the total number of concurrent sessions using UTM features). The TCP proxy code feeds a data stream to the protocol parser which, in turn, can decode the protocols supported by UTM, namely FTP, HTTP, SMTP, POP3, and IMAP. The protocol parser extracts the relevant content from each protocol and sends it to the appropriate engine for processing, all of which is depicted in Figure 9-1.

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

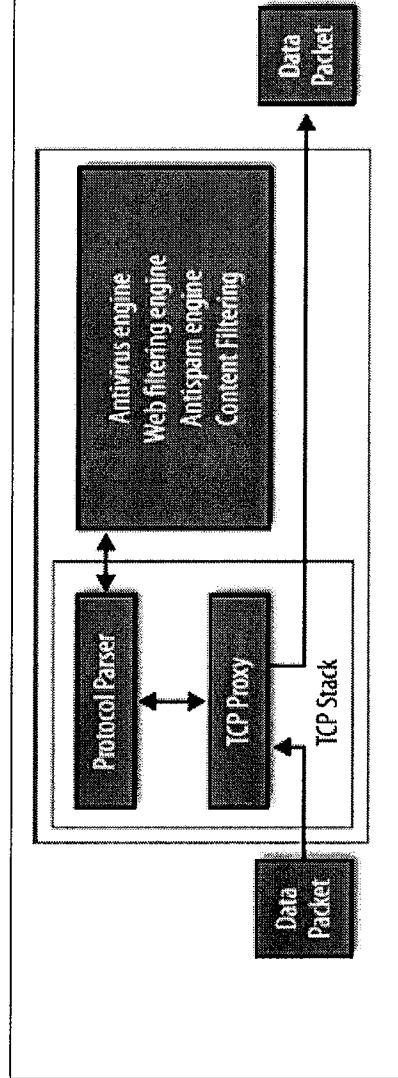


Figure 9-1. How SRX proxies a session

Source: *Junos Security*, By: Rob Cameron; Brad Woodberg; Patricio Giecco; Timothy Eberhard; James Quin; Publisher: O'Reilly Media, Inc. as part of the Juniper Networks Technical Library, September 7, 2010, ISBN-13: 978-1-4493-8171-4, page 489

Evidence '163 C1 1b(16)

As opposed to most appliances that must examine every packet in every session, Dynamic Application Awareness and IPS enable you to identify applications by optionally configuring the software to examine just the first few packets of newly initiated sessions. Once the application is identified, a router-integrated policy manager provisions the forwarding plane (in real time) with the appropriate session handling instructions (such as, block, rate limit, apply CoS, etc).

The forwarding plane resources then ensure that the session is treated and forwarded in accordance with the policy, and the service plane resources can be allocated to other sessions, permitting the solution to scale with high performance. Traffic flows through the Dynamic Application Awareness and the IPS processes as

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

follows (Figure 3).

1. The subscriber initiates a session.
2. Dynamic Application Awareness: The session is forwarded to the Dynamic Application Awareness engine hosted on the MS-PIC/MS-DPC. IPS: The session is forwarded to the IPS engine hosted on the MS-PIC/MS-DPC.
3. Dynamic Application Awareness: The packet header is searched to identify the application based on its port, address, or signature. IPS: The packet is searched to identify threats and attacks using the following detection mechanisms.
 - Anomaly—check traffic against protocol standard.
 - Signature—protocol-aware context signature.
 - Backdoor—detect traffic bypassing normal authentication procedures.
4. The application policy request is forwarded to a local policy manager.
5. The local policy manager compares the identified application against a customer-defined list of application handling instructions. By default, all packets in the session are examined. One user-configurable option is that the session incurs no further analysis. In this case, Dynamic Application Awareness or IPS no longer analyzes this session, and its resources are available to analyze other sessions. Otherwise, the traffic is pushed to the forwarding plane (step 6).
6. **The local policy manager provisions the appropriate enforcement functions on the forwarding plane in real time.**
 - Rate limit traffic, packet drop
 - Classify traffic (DSCP mark for CoS handling)
 - Connection close, block traffic
 - Statistic gathering and logging

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

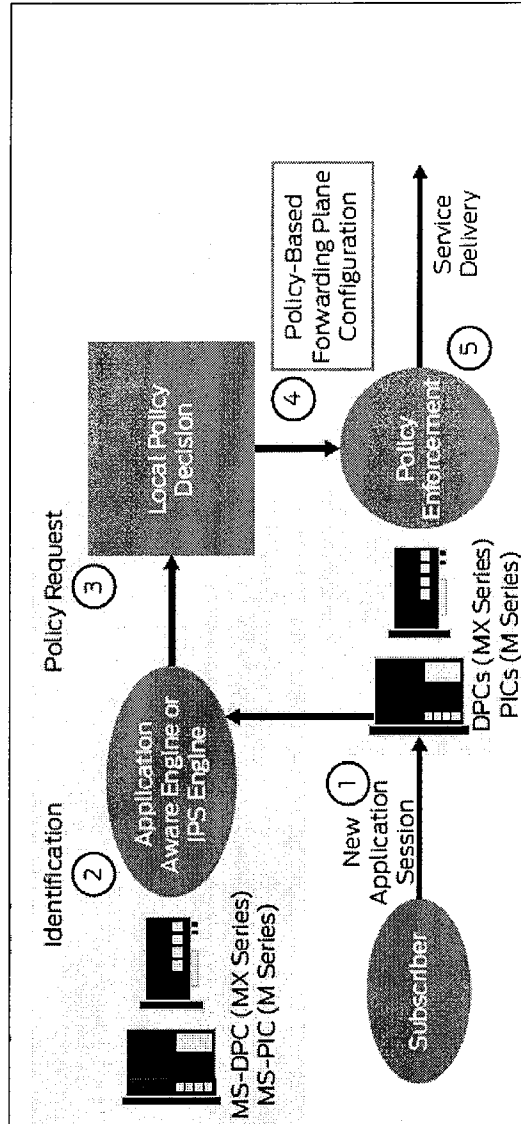


Figure 3: Logical packet flow

Source: *GENERATING NEW REVENUE STREAMS AND INCREASING NETWORK SECURITY Dynamic Application Awareness and Intrusion Prevention System*, Published by Juniper Networks, Dec, 2009, www.juniper.net/us/en/local/pdf/whitepapers/2000339-cn.pdf

Evidence '163 C1 1b(17)

Not Just Another Chassis Design

The Dynamic Services Architecture is based on a chassis design; however, it is a complete departure from traditional chassis architecture. Rather than simply providing a fast backplane, the Dynamic Services Architecture includes the management and control necessary to incorporate individual blades into a powerful collective solution. Rather than housing disparate cards, the Dynamic Services Architecture adds each blade

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

	<p>into a growing pool of resources. These resources can then be utilized as necessary for optimal processing of network traffic.</p> <p>Switch Fabric, Control Board and Route Engine</p> <p>At the heart of the Dynamic Services Architecture is the Switch fabric and Control Board (SCB). The SCB transforms the chassis from a simple blade enclosure into a highly effective mesh network. The purpose of the SCB is to allow all blades in the chassis to send traffic at extremely high bandwidth.</p> <p>The Route Engine (RE) is tightly coupled with the functionality of the SCB and can be considered the central nervous system of the architecture. The RE is the control plane of the chassis and provides overall management and communications to and from system administrators, as well as calculating route tables for routing network traffic.</p> <p>The operating system, which includes key chassis functionality, also runs on the RE. In the case of networking and security, functionalities such as advanced routing, switching, flow-base security, zone-based management, and screens are available on the OS.</p> <p>Service Processing Cards</p> <p>If the RE is the central nervous system of the chassis, the Service Processing Card (SPC), is the brain. SPCs are blades that provide the capacity to perform the heavy lifting of processing network packets.</p> <p>Session Distribution</p> <p>The Dynamic Services Architecture also supports automatic load balancing with advanced performance and capacity due to its session distribution design. This is enabled by the intelligent input/output and network processing subsystems, which balance sessions across the shared pool of SPCs (the "brain" discussed above). This is possible because all the SPCs in the system run the same services and have the same configuration. There is no specific mapping from one IOC to one SPC; rather, each flow is mapped dynamically upon session creation.</p>
--	---

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

	<p>Any session coming in any port can be forwarded, on a session-by-session basis, to any SPC in the system.</p> <p>This load balancing is performed automatically, with no configuration or oversight by the system administrator. This is dramatically opposed to traditional chassis-based solutions, where each processing blade is an independent firewall, with its own dedicated traffic, unique configuration, and routing support.</p> <p>Packet Flow</p> <p>In the same way, the packet flow within the Dynamic Services Architecture becomes fully integrated and far easier to manage. No longer is it necessary for administrators to provide separate instructions to each blade for traffic management. Each packet traversing the system now takes the same basic path:</p> <ol style="list-style-type: none"> 1. The ingress packet enters Ethernet port on the IOC. 2. It is processed by the IOC and passed to the switch fabric. 3. One processing unit on the SPC receives and processes the packet for the firewall, IPsec VPN, and/or IPS. If the packet is to be dropped, the SPC does so and will typically log the event. 4. If the packet is to be passed, it is passed back through the switch fabric to the IOC, where it is processed by the IOC processor, where QoS is applied if necessary. 5. The packet is then passed out the Ethernet port to egress the system.
--	---

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

	<p style="text-align: center;">Figure 2: An example of a fully integrated packet flow (SRX5000 line)</p> <p>Source: <i>Dynamic Services Architecture: a Revolutionary Approach to Integrated Network Security</i>, published by Juniper Networks, Oct 2009, pages 4-6, https://www.juniper.net/us/en/local/pdf/whitepapers/2000288-en</p>
<p>1c. wherein dynamically identifying includes selecting individual components to create the nonpredefined sequence of components after the first packet is received;</p>	<p>The accused products utilize a technique of "policy expression", which are script-like directives that are loaded and re-loaded into the systems while they are running. They may be loaded and re-loaded into the systems by people, other systems or software, or both. The policies direct the system to identify the processing components and algorithms which are to be applied to the network traffic which is classified through packet inspection.</p> <p>The accused products identify a packet, look at the latest loaded and resolved policy expression which applies to that traffic/application flow, and then arrange a sequence of processing components to affect the policy expression directive. The system will contain a large library of processing components. Fully custom traffic/application flow</p>

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

specifications, as well as fully custom processing components, can be dynamically loaded and re-loaded into the system as well.

Evidence '163 C1 1c(1)

To secure your network from new viruses and attacks, your security solution must offer multiple attack detection methods and an efficient way to use the various capabilities.

To stay one step ahead of these attacks, you need a solution that can adapt to ever-changing security threats and allow you to do so with minimal effort.

Juniper Networks IDP Series Intrusion Detection and Prevention Appliances with Multi-Method Detection (MMD), offers comprehensive coverage by leveraging multiple detection mechanisms. For example, by utilizing signatures, as well as other detection methods including protocol anomaly traffic anomaly detection, the Juniper Networks IDP Series appliances can thwart known attacks as well as possible future variations of the attack.

Backed by Juniper Networks Security Lab, signatures for detection of new attacks are generated on a daily basis, working very closely with many software vendors.

While an IDP solution is a critical component of every enterprise security infrastructure, it also offers the benefit of streamlining your business based on the applications used in the network. In addition to identifying viruses and attacks, the Juniper Networks IDP Series can identify the application associated with the particular traffic. Application intelligence enables accurate detection and reporting of volume used by applications such as social networking, peer-to-peer, or instant messaging. Armed with the knowledge of these applications running in the network, administrators can easily manage them by limiting bandwidth, restricting their use, or changing their prioritization for the best network optimization.

By accurately identifying and prioritizing application traffic, enterprises can ensure the necessary network bandwidth for business-critical applications without banning or blocking non-business applications. If necessary, specific application traffic can be blocked altogether to meet business or regulatory compliance.

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

Source: *IDP Series Intrusion Detection and Prevention Appliances*, published by Juniper Networks, Oct 2009, <http://www.juniper.net/us/en/local/pdf/brochures/1500025-en.pdf>

Evidence '163 C1 1c(2)

A security policy, which can be configured from the user interface, controls the traffic flow from one zone to another zone by defining the kind(s) of traffic permitted from specified IP sources to specified IP destinations at scheduled times.

Policies allow you to **deny, permit, reject** (deny and send a TCP RST or ICMP port unreachable message to the source host), **encrypt and decrypt, authenticate, prioritize, schedule, filter**, and **monitor** the traffic attempting to cross from one security zone to another. You decide which users and what data can enter and exit, and **when and where** they can go.

Source: *Junos OS Security Configuration Guide, Juniper Networks, May 2010, Page 146*, <https://www.juniper.net/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-security/junos-security-swconfig-security.pdf>

Evidence '163 C1 1c(3)

There can be many dozens—or even thousands—of policies configured in various SRX devices (this number varies by platform). When packets ingress any of the devices, they are evaluated against security policies.

If a match is found then the SRX does what it was instructed to do with those packets and stops evaluating through the rest of the policies.

Security policies are at the heart of any of the firewall functions of the SRX Services Gateway platform. By default, traffic entering an interface destined to any address is going to be blocked. This is the expected default behavior, and no traffic is allowed through the SRX until you permit it to enter by using security policies.

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

	<p>Policy configuration entitles an IF-THEN-ELSE algorithm: IF traffic X is matched, THEN action Y is performed, ELSE drop packet (default behavior).</p> <p>Matching traffic (IF statement) consists of looking at packets for the five following elements:</p> <ol style="list-style-type: none"> 6. Source zone: the predefined or custom zone created from the perspective of the SRX that you are configuring. 7. Source IP: any IP address, or an address book, that specifies a host IP, or a subnet. The source selected has to match the source zone. 8. Destination zone: predefined or custom zone created from the perspective of the SRX that you are configuring. 9. Destination IP: any IP address, or an address book that specifies a host IP, or a subnet. The destination selected has to match the destination zone. 10. Application: predefined or custom service that defines the source/destination ports, protocol involved, and timeout value. <p>If an incoming packet matches all the previous five elements, the action (THEN statement) defines what to do with this or any other packets matching the same combination:</p> <ul style="list-style-type: none"> • deny: drops the packet (silently). • reject: drops the packet and sends a TCP-Reset to the originator of the traffic. • permit: permits the packet. • log: instructs the SRX to create a log entry for matching packets. • count: provides accounting information per session. <p>Source: <i>Day One: Deploying SRX Series Services Gateways, Junos Dynamic Services Series</i>, published by Juniper Networks, Jan 2011, pages 54, 55, http://www.juniper.net/us/en/community/junos/training-certification/day-one/dynamic-services-series/deploying-srx-series/</p> <p>The accused products not only support the “firewall” types of policies mentioned above, but they support much more complicated IDP policies. IDP policies are sometimes called “rulebases” and the traffic classification specification used to match a rulebase is often called a “signature” to reflect their more general programmability.</p>
--	---

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

Evidence '163 C1 1c(4)

To help block malicious application-level attacks, Juniper Networks seamlessly integrates intrusion prevention across the entire product line. For central enterprise sites, data center environments and service provider networks with high volumes of throughput, the Juniper Networks ISG Series Integrated Security Gateways with IPS, Juniper Networks SRX100, SRX210, SRX220, SRX240, SRX650, SRX1400, SRX3000 line and SRX5000 line of services gateways can be deployed for application-level protection. The ISG Series and SRX Series tightly integrates the same software found on the Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to provide unmatched application-level protection against worms, trojans, spyware, and malware. More than 60 protocols are recognized including those used by advanced applications such as VoIP and streaming media.

Unmatched security processing power and network segmentation features protect critical high-speed networks against the penetration and proliferation of existing and emerging application-level threats. With multiple attack detection mechanisms, including stateful signatures and protocol anomaly, the ISG Series and SRX Series Services Gateways performs in-depth analysis of application protocol, context, state and behavior to deliver Zero-day protection.

Security administrators can deploy Juniper Networks AppSecure capability using deep inspection to block application-level attacks before they infect the network and inflict any damages. AppSecure utilizes advanced, high-performance detection mechanisms integrated with stateful inspection firewall, along with multiple threat inspection engines operating in parallel to accurately detect advanced persistent threats, including those found in nested applications within applications.

Source: *Integrated Firewall/VPN Platforms*, published by Juniper Networks, Nov. 2010, <http://www.juniper.net/us/en/local/pdf/brochures/1500024-en.pdf>

Evidence '163 C1 1c(5)

The IDP rulebase employs an attack object database to support two robust detection methods: stateful signatures and protocol anomalies.

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

A stateful signature combines an attack pattern with service, context, and other properties into a signature attack object. As a result, the IDP system does not need to expend resources inspecting huge sections of network traffic where attacks cannot possibly be, and IDP produces very few false positives.

A protocol anomaly is a deviation from protocol standards established by the Internet Engineering Taskforce (IETF) Request for Comment (RFC) process. Traffic that does not adhere to these standards is suspicious because most legitimate applications adhere to the standards, and anomalies can fairly be regarded as purposeful attempts to evade an intrusion detection system (IDS). IDP protocol-anomaly attack objects find traffic that deviates from IETF RFC standards.

When you create rules for the IDP rulebase, you specify:

- A source/destination/service match condition
- Attack objects
- Action
- Notification options

The IDP engine inspects the session beginning with the first packet to determine whether the session matches a rule. If the session matches all rule settings for source, destination, service, and VLAN tag ID, the IDP system decodes the traffic and inspects the session packets for the attack objects specified in the rule.

Source: *IDP Series Concepts and Examples Guide, Juniper Networks, Published Feb. 2011*, http://www.juniper.net/techpubs/en_US/idp5.1/information-products/topic-collections/idp-5-1-1-concepts-examples.pdf, pages 91, 92

Unified Threat Management (UTM) is a term used to describe the consolidation of several security features into one device, protecting against multiple threat types.

Evidence '163 C1 1c(6)

The security features provided as part of the UTM solution are:

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

- **Antispam**—E-mail spam consists of unwanted e-mail messages, usually sent by commercial, malicious, or fraudulent entities. The antispam feature examines transmitted e-mail messages to identify e-mail spam. When the device detects an e-mail message deemed to be spam, it either drops the message or tags the message header or subject field with a preprogrammed string. The antispam feature uses a constantly updated spam block list (SBL). Sophos [n.b., an outside company accessed through an algorithm which goes to a special internet site], updates and maintains the IP-based SBL.
- **Full File-Based Antivirus**—A virus is executable code that infects or attaches itself to other executable code to reproduce itself. Some malicious viruses erase files or lock up systems. Other viruses merely infect files and overwhelm the target host or network with bogus data. The full file-based antivirus feature provides file-based scanning on specific Application Layer traffic checking for viruses against a virus signature database. It collects the received data packets until it has reconstructed the original application content, such as an e-mail file attachment, and then scans this content.
- **Express Antivirus**—Express antivirus scanning is offered as a less CPU intensive alternative to the full file-based antivirus feature. The express antivirus feature, like the full antivirus feature, scans specific Application Layer traffic for viruses against a virus signature database. However, unlike full antivirus, express antivirus does not reconstruct the original application content. Rather, it just sends (streams) the received data packets, as is, to the scan engine. With express antivirus, the virus scanning is executed by a hardware pattern matching engine. This improves performance while scanning is occurring, but the level of security provided is lessened.
- **Content Filtering**—Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type.
- **Web Filtering**—Web filtering lets you manage Internet usage by preventing access to inappropriate Web content.

Before you can configure most UTM features, you must first configure the custom objects for the feature in question. Custom objects are global parameters for UTM features. This means that configured custom objects can be applied to all UTM policies where applicable, rather than only to individual policies.

Source: *Junos OS Security Configuration Guide, Juniper Networks, May 2010, Page 843-844*, <https://www.juniper.net/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-security/junos-security-swconfig-security.pdf>

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

Evidence '163 C1 1c(7)

Once a security policy specifies a UTM policy, a transparent proxy processes all matching traffic and, in the case of this book's SRX devices, modifies the contents of the traffic or generate error messages back to the user. To proxy a session, an SRX device acts both as a TCP client and as a server terminating and originating a TCP session. This uses significant resources, in terms of both memory and CPU, which puts some constraints on the total number of sessions an SRX can proxy (and, in turn, the total number of concurrent sessions using UTM features). The TCP proxy code feeds a data stream to the protocol parser which, in turn, can decode the protocols supported by UTM, namely FTP, HTTP, SMTP, POP3, and IMAP. The protocol parser extracts the relevant content from each protocol and sends it to the appropriate engine for processing, all of which is depicted in Figure 9-1.

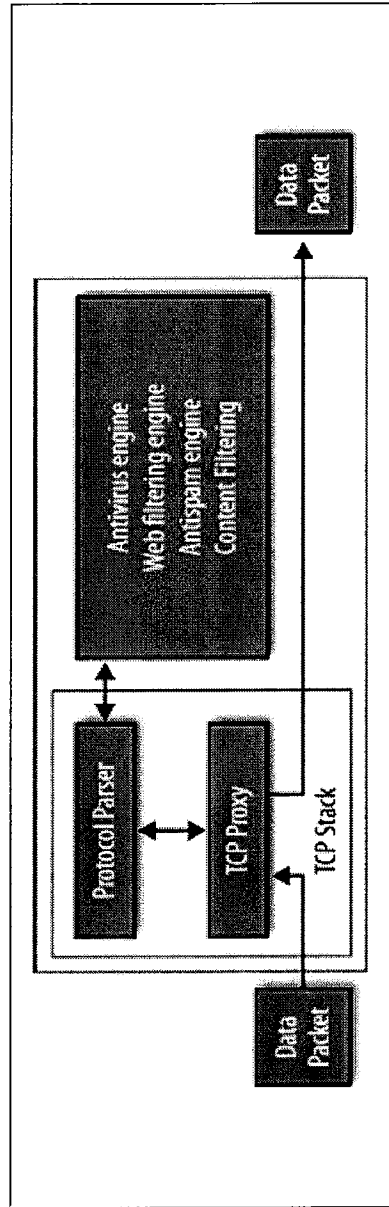


Figure 9-1. How SRX proxies a session

Source: *Junos Security*, By: Rob Cameron; Brad Woodberg; Patricio Giecco; Timothy Eberhard; James Quin; Publisher: O'Reilly Media, Inc. as part of the Juniper Networks Technical Library, September 7, 2010, ISBN-13: 978-1-4493-8171-4, page 489

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

Juniper employs what it calls "the Dynamic Services Architecture". This architecture dynamically arranges and connects the needed components to implement the security processing identified first by the classification, and then by the policy directives.

Evidence '163 C1 1c(8)

As opposed to most appliances that must examine every packet in every session, Dynamic Application Awareness and IPS enable you to identify applications by optionally configuring the software to examine just the first few packets of newly initiated sessions. Once the application is identified, a router-integrated policy manager provisions the forwarding plane (in real time) with the appropriate session handling instructions (such as, block, rate limit, apply CoS, etc).

The forwarding plane resources then ensure that the session is treated and forwarded in accordance with the policy, and the service plane resources can be allocated to other sessions, permitting the solution to scale with high performance. Traffic flows through the Dynamic Application Awareness and the IPS processes as follows (Figure 3).

7. The subscriber initiates a session.
8. Dynamic Application Awareness: The session is forwarded to the Dynamic Application Awareness engine hosted on the MS-PIC/MS-DPC. IPS: The session is forwarded to the IPS engine hosted on the MS-PIC/MS-DPC.
9. Dynamic Application Awareness: The packet header is searched to identify the application based on its port, address, or signature. IPS: The packet is searched to identify threats and attacks using the following detection mechanisms.
 - Anomaly—check traffic against protocol standard.
 - Signature—protocol-aware context signature.
 - Backdoor—detect traffic bypassing normal authentication procedures.
10. The application policy request is forwarded to a local policy manager.

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

11. The local policy manager compares the identified application against a customer-defined list of application handling instructions. By default, all packets in the session are examined. One user-configurable option is that the session incurs no further analysis. In this case, Dynamic Application Awareness or IPS no longer analyzes this session, and its resources are available to analyze other sessions. Otherwise, the traffic is pushed to the forwarding plane (step 6).

12. The local policy manager provisions the appropriate enforcement functions on the forwarding plane in real time.

- Rate limit traffic, packet drop
- Classify traffic (DSCP mark for CoS handling)
- Connection close, block traffic
- Statistic gathering and logging

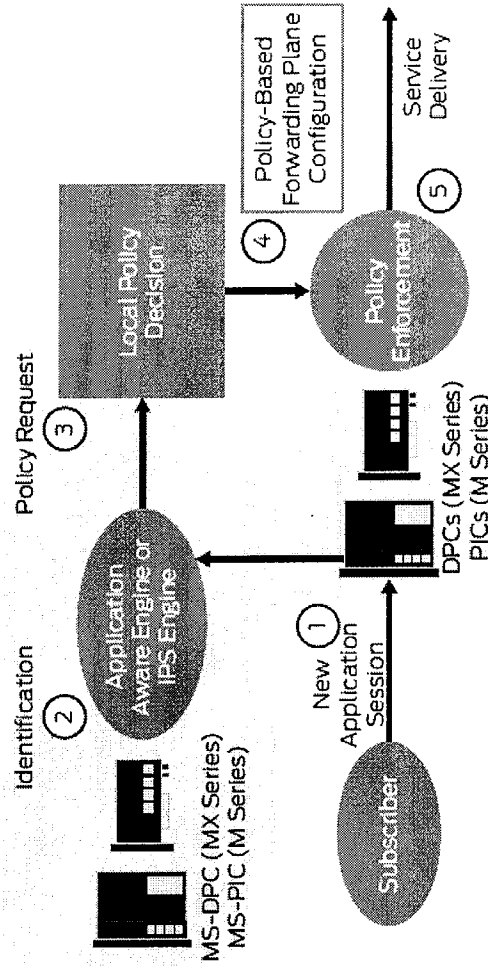


Figure 3: Logical packet flow

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

Source: *GENERATING NEW REVENUE STREAMS AND INCREASING NETWORK SECURITY Dynamic Application Awareness and Intrusion Prevention System*, Published by Juniper Networks, Dec, 2009, www.juniper.net/us/en/local/pdf/whitepapers/2000339-en.pdf

Evidence '163 C1 1c(9)

Not Just Another Chassis Design

The Dynamic Services Architecture is based on a chassis design; however, it is a complete departure from traditional chassis architecture. Rather than simply providing a fast backbone, the Dynamic Services Architecture includes the management and control necessary to incorporate individual blades into a powerful collective solution. Rather than housing disparate cards, the Dynamic Services Architecture adds each blade into a growing pool of resources. These resources can then be utilized as necessary for optimal processing of network traffic.

Switch Fabric, Control Board and Route Engine

At the heart of the Dynamic Services Architecture is the Switch fabric and Control Board (SCB). The SCB transforms the chassis from a simple blade enclosure into a highly effective mesh network. The purpose of the SCB is to allow all blades in the chassis to send traffic at extremely high bandwidth.

The Route Engine (RE) is tightly coupled with the functionality of the SCB and can be considered the central nervous system of the architecture. The RE is the control plane of the chassis and provides overall management and communications to and from system administrators, as well as calculating route tables for routing network traffic.

The operating system, which includes key chassis functionality, also runs on the RE. In the case of networking and security, functionalities such as advanced routing, switching, flow-base security, zone-based management, and screens are available on the OS.

Service Processing Cards

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

If the RE is the central nervous system of the chassis, the Service Processing Card (SPC), is the brain. SPCs are blades that provide the capacity to perform the heavy lifting of processing network packets.

Session Distribution

The Dynamic Services Architecture also supports automatic load balancing with advanced performance and capacity due to its session distribution design. This is enabled by the intelligent input/output and network processing subsystems, which balance sessions across the shared pool of SPCs (the "brain" discussed above). This is possible because all the SPCs in the system run the same services and have the same configuration. There is no specific mapping from one IOC to one SPC; rather, each flow is mapped dynamically upon session creation.

Any session coming in any port can be forwarded, on a session-by-session basis, to any SPC in the system.

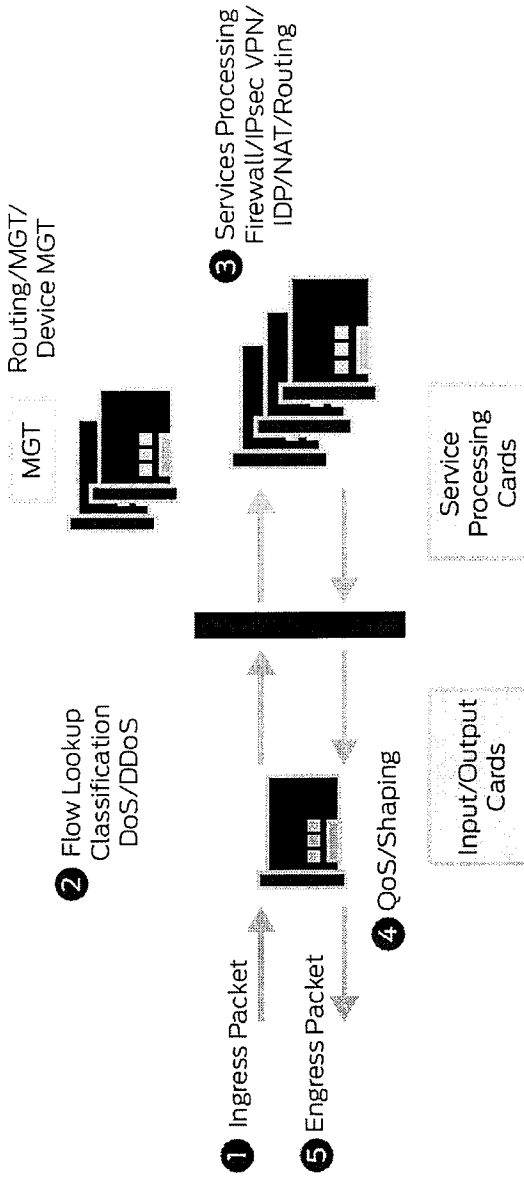
This load balancing is performed automatically, with no configuration or oversight by the system administrator. This is dramatically opposed to traditional chassis-based solutions, where each processing blade is an independent firewall, with its own dedicated traffic, unique configuration, and routing support.

Packet Flow

In the same way, the packet flow within the Dynamic Services Architecture becomes fully integrated and far easier to manage. No longer is it necessary for administrators to provide separate instructions to each blade for traffic management. Each packet traversing the system now takes the same basic path:

1. The ingress packet enters Ethernet port on the IOC.
2. It is processed by the IOC and passed to the switch fabric.
3. One processing unit on the SPC receives and processes the packet for the firewall, IPsec VPN, and/or IPS. If the packet is to be dropped, the SPC does so and will typically log the event.
4. If the packet is to be passed, it is passed back through the switch fabric to the IOC, where it is processed by the IOC processor, where QoS is applied if necessary.
5. The packet is then passed out the Ethernet port to egress the system.

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

	 <p style="text-align: center;">Figure 2: An example of a fully integrated packet flow (SRX5000 line)</p> <p>Source: <i>Dynamic Services Architecture: a Revolutionary Approach to Integrated Network Security</i>, published by Juniper Networks, Oct 2009 , pages 4-6, https://www.juniper.net/us/en/local/pdf/whitepapers/2000288-en</p>
<p>1d. and storing an indication of each of the identified components so that the nonpredefined sequence does not need to be re-identified for subsequent packets of the</p>	<p>The accused products store information about the processing components, along with a correlation to the network traffic that those components are to operate on, as defined by the result of the non-predetermined result of the packet classification definitions, the network flows, and the executed policy directives, in accordance with this limitation.</p> <p>Evidence '163 C1 1d(1)</p> <p>The security policy to be used for the first packet of a flow is cached in a flow table for use with the same</p>

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

message;	<p>flow and closely related flows. Security policies are associated with zones. A zone is a collection of interfaces that define a security boundary. A packet's incoming zone, as determined by the interface through which it arrived, and its outgoing zone, as determined by the forwarding lookup, together determine which policy is used for packets of the flow.</p> <p>Source: <i>Junos OS Security Configuration Guide</i>, Published by Juniper Networks, Inc., March 2011, page 4, https://www.juniper.net/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-security/junos-security-swconfig-security.pdf</p> <p>Evidence '163 C1 1d(2)</p> <p>Flow-based packet processing, which is stateful, requires the creation of sessions. A session is created for the first packet of a flow for the following purposes:</p> <ul style="list-style-type: none"> • To store most of the security measures to be applied to the packets of the flow. • To cache information about the state of the flow. <p>For example, logging and counting information for a flow is cached in its session. (Some stateful firewall screens rely on threshold values that pertain to individual sessions or across all sessions.)</p> <ul style="list-style-type: none"> • To allocate required resources for the flow for features such as NAT. • To provide a framework for features such as ALGs and firewall features <p>Most packet processing occurs in the context of a flow, including:</p> <ul style="list-style-type: none"> • Management of policies, NAT, zones, and most screens. • Management of ALGs and authentication. <p>Source: <i>Junos OS Security Configuration Guide</i>, Published by Juniper Networks, Inc., March 2011, page 6, https://www.juniper.net/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-security/junos-security-swconfig-security.pdf</p>
1e. and for each of a	<p>The accused products maintain state, by flow, and explained in the introductory narrative, above.</p>

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

<p>plurality of packets of the message in sequence, for each of a plurality of components in the identified non-predefined sequence, retrieving state information relating to performing the processing of the component with the previous packet of the message;</p>	<p><u>Evidence '163 C1 1e(1)</u></p> <p>When the application identification feature identifies a new application, it caches the result (the destination address, port, protocol, and service) to reduce processing for subsequent sessions. The application cache and extended application cache are maintained separately.</p> <p>Source: <i>IDP Series Concepts and Examples Guide</i>, Published by Juniper Networks, Feb. 2011, Page 96, http://www.juniper.net/techpubs/en_US/ldp5.1/information-products/topic-collections/ldp-5-1-r1-concepts-examples.pdf</p> <p><u>Evidence '163 C1 1e(2)</u></p> <p>The fast-path packet process consists of the following steps:</p> <ol style="list-style-type: none"> 1. An inbound packet is received by an interface and sent to the NPU, which provides processing for that interface. The NPU performs a session lookup and determines that it knows the session and the SPU processing it. The NPU then forwards the packet directly to the SPU which owns the session. 2. Policing, stateless filtering, and screens are performed. Technically, the screens that are applied after the initial packet setup are all on the NPU on the high-end SRX platforms. 3. The SPU determines if it knows about the session already, which in this case it does. The session entry will provide cached instructions on how to process the packet so that the SRX does not have to do any forwarding or policy checks, as these have already been determined in the first packet processing. <p>Source: <i>Junos Security</i>, By: Rob Cameron; Brad Woodberg; Patricio Giecco; Timothy Eberhard; James Quin; Publisher: O'Reilly Media, Inc. as part of the Juniper Networks Technical Library, September 7, 2010, ISBN-13: 978-1-4493-8171-4, page 724</p>
<p>If performing the processing of the identified component with the packet and the</p>	<p>The accused product performs the processing based on the retrieved state information.</p> <p><u>Evidence '163 C1 1f(1)</u></p>

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

retrieved state information;	<p>When the IDP engine processes security policy rules, it examines the session, beginning with the first packet, to identify a match. To match service or application, the IDP engine first compares the session against the application identification cache to identify the application. If the session does not match the application identification cache, the IDP engine processes the session against the application signatures. If the IDP engine is still unable to determine the application, it uses the standard application protocol and port.</p> <p>Source: <i>IDP Series Concepts and Examples Guide, Juniper Networks, Published Feb. 2011</i>, http://www.juniper.net/techpubs/en_US/ldp5.1/information-products/topic-collections/ldp-5-1-r1-concepts-examples.pdf, page 96</p>
lg. and storing state information relating to the processing of the component with the packet for use when processing the next packet of the message.	<p>State information is stored, as described in the Technical Narrative, above.</p> <p>Evidence '163 C1 1g(1)</p> <p>Application system cache (ASC) saves the mapping between an application type and the corresponding destination IP address, destination port, protocol type, and service.</p> <p>Once an application is identified, its information is saved in the cache so that only one pattern matching is required for an application running on a particular system, thereby expediting the identification process. A mapping is saved in the cache only if the matched signature contains both client-to-server and server-to-client patterns. This process protects the system from hackers who might send malicious packets through a legitimate server port so that it is interpreted as a different application.</p> <p>By default, the application system cache saves the mapping information for 3600 seconds. However, you can configure the cache timeout value.</p> <p>Source: <i>Junos OS Security Configuration Guide</i>, Published by Juniper Networks, Inc., March 2011, page 802, https://www.juniper.net/techpubs/software/junos-security/junos-security10.2/junos-security-swconfig-security/junos-security-swconfig-security.pdf</p> <p>Additionally, the accused products can discover their own view of the baseline security state of the network, store this</p>

Implicit Networks, Inc.
U.S. Patent No. 6,629,163 C1
Claims Chart
Implicit Networks, Inc. v. Juniper Networks, Inc.
Security: Flow Based Processing

state, and automatically develop security policies to detect and act on behavior which varies from that baseline.

Evidence '163 C1 1g(2)

The Profiler is a network-analysis tool that helps you learn about your internal network so you can create effective security policies and minimize unnecessary log records. The Profiler queries and correlates information from multiple IDP Series devices.

After you configure the Profiler, it **automatically learns about your internal network** and the elements that constitute it, including hosts, peers (which host is talking to which other host), ports (non-IP protocols, TCP/UDP ports, RPC programs), and Layer 7 data that uniquely identifies hosts, applications, commands, users, and filenames. You can use this data to investigate and analyze potential problems in the network and to resolve security incidents.

During profiling, the IDP Series device records network activity at Layer 3, Layer 4, and Layer 7 and stores this information in a searchable database called the Profiler DB. The Profiler uses session creation, session teardown, and protocol contexts to generate this database, which defines all unique activities occurring on your network. Unique activities include attempts, probes, and successful connections. The device logs normal events only once, and it logs all unique events as often as they occur.

Baseline data gives you the building blocks for your network security policy.

After you have created a baseline and installed an appropriate security policy, you can use Profiler to alert you when new hosts or applications appear in your network. You can analyze the alerts to decide whether to update your security policy.

Source: *IDP Series Concepts and Examples Guide, Juniper Networks, Published Feb. 2011*, http://www.juniper.net/techpubs/en_US/idp5.1/information-products/topic-collections/idp-5-1-r1-concepts-examples.pdf, page 32